



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/778,623	02/06/2001	Cheuk W. Ko	NA00-12101	9616

28875 7590 09/28/2004

Zilka-Kotab, PC  
P.O. BOX 721120  
SAN JOSE, CA 95172-1120

EXAMINER

CHAI, LONGBIT

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 09/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/778,623

Applicant(s)

KO, CHEUK W.

Examiner

Longbit Chai

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 09 June 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☐ Claim(s) \_\_\_\_\_ is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 February 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

### *Priority*

1. No claim for priority has been made in this application.
2. The effective filing date for the subject matter defined in the pending claims in this application is 02/06/2001.

### ***Claim Rejections - 35 USC § 102***

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 3 – 4, 9, 11 – 12, 17 and 19 – 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Warrender ("Detection Intrusions Using System Calls: Alternative Data Models" IEEE Computer Society, Symposium on Security and Privacy, 1999, 133 – 145), hereinafter referred to as Warrender.
4. As per claim 1, 9, and 17, Warrender teaches a method for automatically generating a valid behavior specification for use in an intrusion detection system for a computer system, comprising:
  - a. receiving an exemplary set of system calls that includes positive examples of valid system calls, and possibly negative examples of invalid system calls (Warrender: see for example, Section 1.0 Line 2 – 13); and

b. automatically constructing the valid behavior specification from the exemplary set of system calls by selecting a set of rules covering valid system calls (Warrender: see for example, Section 5.3 Line 42 – 43: A list of rules is qualified as a behavior specification);

c. wherein the set of rules covers all positive examples in the exemplary set of system calls without covering negative examples (Warrender: see for example, Section 5.3 Line 19 – 21);

d. wherein selecting a rule for the valid behavior specification involves using an objective function that seeks to maximize the number of positive examples covered by the rule while seeking to minimize the number of possible system calls covered by the rule (Warrender: see for example, Section 5.3 Line 42 – 50 and 5.3 Line 2 – 24).

5. As per claim 3, 11 and 19, Warrender teaches the claimed invention as described above (see claim 1, 9 and 17 respectively). Warrender further teaches the objective function additionally seeks to minimize a length of the rule (Warrender: see for example, Section 5.3 Line 1 – 4 and 5.3 Line 22 – 24).

6. As per claim 4, 12 and 20, Warrender teaches the claimed invention as described above (see claim 1, 9 and 17 respectively). Warrender further teaches monitoring an executing program by: receiving a system call generated by the executing program (Warrender: see for example, Section 2.1 Line 9 – 11); determining whether the system call is covered by a rule from within the valid behavior specification (Warrender: see for example, Section 2.3 Line 4 – 14 and Section 5.3 Line 42 – 43);

Art Unit: 2131

and if the system call is not covered by a rule from within the valid behavior specification, indicating that the system call is invalid ((Warrender: see for example, Section 2.3 Line 4 – 14 and Section 5.3 Line 42 – 43).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 2, 10 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warrender ("Detection Intrusions Using System Calls: Alternative Data Models", 1999), hereinafter referred to as Warrender, in view of Ko ("Automated Detection of Vulnerabilities in Privileged Programs by Executing Monitoring", 1994), hereinafter referred to as Ko.

8. As per claim 2, 10 and 18, Warrender teaches the claimed invention as described above (see claim 1, 9 and 17 respectively). Warrender does not teach the objective function additionally seeks to minimize the number of privileged system calls covered by the rule.

9. Ko teaches the objective function additionally seeks to minimize the number of privileged system calls covered by the rule (Ko: see for example, Section 8.0 Line 30 – 33).

Art Unit: 2131

10. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ko within the system of Warrender because Warrender teaches detecting intrusions using system calls and Ko teaches intrusion detection by monitoring the execution of privileged programs (Ko: see for example, Abstract).

11. Claims 5 – 6, 13 – 14 and 21 – 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warrender ("Detection Intrusions Using System Calls: Alternative Data Models", 1999), hereinafter referred to as Warrender, in view of Hofmeyr ("Intrusion Detection using Sequence of System Calls", 1998), hereinafter referred to as Hofmeyr.

12. As per claim 5, 13 and 21, Warrender teaches the claimed invention as described above (see claim 1, 9 and 17 respectively). Warrender does not teach producing the exemplary set of system calls by running an exemplary program and recording system calls generated by the exemplary program.

13. Hofmeyr teaches producing the exemplary set of system calls by running an exemplary program and recording system calls generated by the exemplary program (Hofmeyr: see for example, Page 3 Line 11 – 14).

14. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Hofmeyr within the system of Warrender because Warrender teaches detecting intrusions using system calls and Hofmeyr

teaches detecting intrusions at the level of privileged processes (Hofmeyr: see for example, Abstract).

15. As per claim 6, 14 and 22, Warrender teaches the claimed invention as described above (see claim 1, 9 and 17 respectively). Warrender does not teach the exemplary set of system calls includes calls to functions implemented by an operating system of the computer system.

16. Hofmeyr teaches the exemplary set of system calls includes calls to functions implemented by an operating system of the computer system (Hofmeyr: see for example, Page 11 Line 1 – 2).

17. See same rationale of combination applies here as above in rejecting claim 5.

18. Claims 7 – 8, 15 – 16 and 23 – 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warrender ("Detection Intrusions Using System Calls: Alternative Data Models", 1999), hereinafter referred to as Warrender, in view of Cohen (Patent Number: 5481650), hereinafter referred to as Cohen.

19. As per claim 7, 15 and 23, Warrender teaches the claimed invention as described above (see claim 1, 9 and 17 respectively). Warrender does not teach the set of rules includes at least one Horn clause.

20. Cohen teaches the set of rules includes at least one Horn clause teaches (Cohen: see for example, Column 2 Line 59 – 63).

21. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cohen within the system of Warrender because Warrender teaches detecting intrusions using system calls including a rule induction technique (Warrender: see for example, Abstract Line 11) and Cohen teaches a learning systems that learn by formulating sets of rules from input data and desired responses to such data (Cohen: see for example, Column 1 Line 8 – 10).

22. As per claim 8, 16 and 24, Warrender as modified teaches the claimed invention as described above (see claim 7, 15 and 23 respectively). Warrender as modified further teaches selecting a rule for the valid behavior specification involves:

- a. selecting a positive example from the exemplary set of system calls (Warrender: see for example, Section 1.0 Line 2 – 13);
- b. constructing a Horn clause for the positive example by iterating through a subsumption lattice, starting from a most general possible clause and proceeding to a most specific clause for the positive example, and selecting a Horn clause that maximizes the objective function without covering any negative examples; adding the Horn clause to the set of rules in the valid behavior specification; and removing other positive examples covered by the Horn clause from the exemplary set of system calls, so subsequently selected Horn clauses do not have to cover the other positive examples (Cohen: see for example, Figure 3 and Column 2 Line 59 – 67 and Column 3 Line 1 – 7).



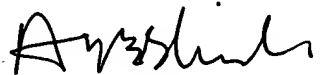
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai  
Examiner  
Art Unit 2131

LBC

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100